2016 IEEE 2nd International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing, IEEE International Conference on Intelligent Data and Security

# Towards Efficient Authentication Scheme with Biometric Key Management in Cloud Environment

Zaid Ameen Abduljabbar[1,2], Hai Jin[1], Zaid Alaa Hussien[1,3], Ali A.Yassin[2],
Mohammed Abdulridha Hussain[1,2], Salah H. Abbdal[1], Deqing Zou[1]
[1]Cluster and Grid Computing Lab, Services Computing Technology and System Lab
School of Computer Science and Technology
Huazhong University of Science and Technology, Wuhan, 430074, China
Email: zaidalsulami@yahoo.com, hjin@hust.edu.cn
[2]University of Basrah, Basrah, Iraq. [3]Southern Technical University, Basrah, Iraq

*Abstract*—**Recently, security issues are obstructing the development and using of cloud computing services. Authentication plays an important role in the cloud security, and numerous concerns have been raised to prevent an unauthorized users to access the entities' resources (sender and receiver) within the cloud environment. Existing solutions are based on one-time authentication scheme, in which a user's password is applicable only for one login session. However, none of the proposed schemes are sufficiently secure to prevent known forms of attack. In addition, these schemes often suffer from significant overhead in the key management.**

**For this reason, we propose a robust one-time authentication scheme based on a non-interactive one-time biometric key to generate one-time login request message. The key used in our scheme has two strong building blocks; that is, it is biometrically based on the extraction of features from the entities' irises, and cryptographically based on the strong key-based message authentication code MAC-SHA-512 and Rivest Cipher 4. The proposed scheme exhibits several important security attributes, such as key agreement, biometric key management, a single authentication request for each user's login, mutual authentication, invulnerability, and efficiency.**

***Keywords—Biometric key management; cloud computing; one-time authentication request; session key agreement***

## I. Introduction

Nowadays, transmitted information has radically increased and has been exponentially distributed [1]. Cloud computing is generally regarded as the computing infrastructure of the next generation [2]. It is an effective means of enabling users to access information-related services and applications from anywhere and at any time [3]. Consequently, more attention should be paid to verify the identity of a user who intends to access resources through the design of a secure authentication mechanism.

Authentication based on password system is the simplest and most traditional authentication mechanism over insecure communications [4]. A static password is basic and the most widely used. Unfortunately, it is also easily guessed, determined through eavesdropping, forgotten, and stolen. Moreover, this method is vulnerable to known attacks such as dictionary, replay, guessing, modification, stolen-verifier, and *denial of service* (DOS) [5].

The probability of known attacks can be reduced by employing an authentication scheme based on a *one-time password* (OTP). In this scheme, a password should be periodically changed [6]. Instead of using static password, each user generates a password that valids only for one login session. Thus, an adversary who successfully intercepts a session key that is used to access a service or to carry out a transaction will learn that the intercepted key is useless given that it is used only once and then discarded. Therefore, OTP access control keys can no longer be reused regardless of whether they are lost on the users end or were stolen by an adversary because these keys change each time a user logs in.

OTP-based authentication methods are usually applied with a key management mechanism that generates a set of the keys, selects the appropriate key for a user's authentication request, and updates the used key to initiate the generation of a new one for later use [5].

Since Lamport [6] brought up the first solution using OTP-based authentication scheme, a number of authors have proposed different subsequent OTP-based authentication schemes to generate a robust login request message. However, most of these schemes suffer from drawbacks in which the key management mechanism is highly complex and requires numerous complicated cryptographic operations; thus, these methods incur high computational costs. In addition, some of these schemes report a high overhead for the authentication messages exchanged between the involved entities, which in turn generates additional communication and transmission costs. Finally, many schemes often encounter problems related to the authentication elements used for user authentication. These elements can categorize the authentication schemes into three types.

The first scheme is based on the token or smart card [7]–[9]. This authentication technique is more powerful than password authentication, but the drawback of the former is the complexity of the user-side device and the fact that the additional card reader required is extra costs. In addition, a smart card or token can be stolen or lost as well [5].

The second scheme requires a password or a personal identification number to initiate the authentication phase [10]. Nonetheless, the weakness of this method is that it does not adequately complicate the guessing of transferred passwords given existing crack techniques.

The third scheme involves either the automated recognition

978-1-5090-2403-2/16 $31.00 © 2016 IEEE
DOI 10.1109/BigDataSecurity-HPSC-IDS.2016.25